UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/578,258	05/04/2006	Masakazu Soga	KAK-0017	1371

23353 7590 09/02/2008

RADER FISHMAN & GRAUER PLLC
LION BUILDING
1233 20TH STREET N.W., SUITE 501
WASHINGTON, DC 20036

EXAMINER
VAUGHAN, MICHAEL R

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
09/02/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/578,258	SOGA ET AL.	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 May 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 2* is/are rejected.

7)☒ Claim(s) *3-7* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 May 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *5-4-06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/578258 filed on 5/4/2006 is presented for examination by the examiner.

Priority

Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been received.

Claim Objections

Claim 6 is objected to because of the following informalities:

Claim 6 is objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claims should refer to other claims in the alternative only. See MPEP § 608.01(n). Accordingly, the claim has not been further treated on the merits.

Allowable Subject Matter

Claims 3-5 and 7 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. The feature of *setting the security mode causes to set the security register and initializes the key counter to 1023 at the same time; and the signature dedicated instruction causes to decrease the key counter by one at the same time when an instruction for conducting signature*

calculation for one bit of the key register, and causes to reset the security mode only when the key counter is 0 resulting from the signature calculation progressing bit by bit has not been found in the search of the prior art.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:
(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim1 is rejected under 35 U.S.C. 103(a) as being unpatentable over USP Application Publication 2002/0095583 to Vanstone et al, hereinafter Vanstone in view of USP 6,298,442 to Kocher et al, hereinafter Kocher.

As per claim 1, Vanstone teaches a secure processor [smart-card], comprising:

a key register including non-volatile memory [RAM] stored with key data (0053);

a key counter configured to indicate a bit position of the key data [values in respective tables] stored in the key register [RAM] to access the key data bit by bit (0097);

a digest register [cyclic shift registers] configured to be stored with digest data to be used for digital signature (0050); and

wherein no path for reading all data out from the outside [remains secret] is prepared for the key register (0053), and the secure processor further comprises a plurality of signature dedicated instructions [programming code] for controlling the key register, the

key counter, and the digest register to obtain a digital signature based on the digest data, as well as general instructions (0050). Vanstone further teaches the need for masking techniques used when generate components of the signature (0060). Vanstone does not explicitly teach a gate configured to output 1 for the content of the digest register when the corresponding bit of the key data accessed by the key counter is 0 and output the content of the digest register as is when the bit of the key data is 1. Kocher teaches the masking technique of a gate configured to output 1 for the content of the digest register when the corresponding bit of the key data accessed by the key counter is 0 and output the content of the digest register as is when the bit of the key data is 1 (col. 5, lines 35-54). Kocher teaches this technique as a means to limit the amount of leakage of protected information including related information that could assist an attacker in gaining more intelligence about a system. Therefore it would have obvious to one of ordinary skill in the art at the time of the invention to use the masking technique of Kocher in the secure processor of Vanstone in order to protect the secret key from being exposed to an attacker. Masking the operation of the digital signature would prevent leakage of the private key which one of ordinary skill in the art knows is the linchpin of the security.

Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combined system of Vanstone and Kocher as applied to claim 1 above, and further in view of USP 6,378,072 to Collins et al, hereinafter Collins.

As per claim 2, Vanstone and Kocher do not explicitly teach a secure processor having a general mode and a security mode as processor running modes;

a security register configured to indicate the security mode; and a general instruction for setting a security mode and a signature dedicated instruction for resetting the same (col. 8, lines 38-44); wherein the general instruction is effective during the general mode while the signature dedicated instruction is effective during the security mode. Collins teaches a general mode [unsecured state] and a security mode [secure state] as processor running modes; a security register [Fig. 4, 412] configured to indicate the security mode; and a general instruction for setting a security mode and a signature dedicated instruction for resetting the same; wherein the general instruction is effective during the general mode while the signature dedicated instruction is effective during the security mode (col. 8, lines 15-18). Collins secure processor is able to operate in two modes depending on the intent of the system. This gives the processor more applications and operation than a processor that can only perform secure operations. Therefore it would have obvious to one of ordinary skill in the art at the time of the invention to modify the combined teaches of Vanstone and Kocher with the teachings of Collins in order to increase the application of the processor. Having a processor which can function in multiple operations cost less than having multiple processors in the system. One of ordinary skill in the art would know the importance of processors and the engineering considerations such as cost, size, and processing power.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

During examination of the instant application a published document by the inventors was found which stated that they had developed secure processors SEP-4, SEP-5, and SEP-6. Applicant cited on the IDS statement the publication of the document detailing SEP-5, which is believed by the Examiner to be the same processor disclosed in the instant application. Examiner requests any publication known to the inventors of SEP-4 which may be pertinent as prior art to the instant application.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business

Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2131

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2131